Verificación en Alloy de modelos y metamodelos específicos del dominio

Ana Garis[1], Alejandro Sánchez[1]

[1] Universidad Nacional de San Luis
Ejército de los Andes 950, San Luis, Argentina
{agaris, asanchez}@unsl.edu.ar

Resumen

La verificación de modelos de sistemas de software es una actividad clave para mejorar la calidad del producto final.

Numerosos lenguajes específicos del dominio han sido creados para favorecer la definición de modelos ajustados a un dominio o área particular. Sin embargo, la verificación de estos modelos, frecuentemente es dejada de lado como actividad complementaria al modelado.

Esta línea de investigación, desarrollo e innovación se orienta a generalizar un mecanismo basado en Alloy, para la especificación y verificación de modelos y metamodelos específicos del dominio. Alloy es un lenguaje formal, soportado por una amigable herramienta de verificación y validación. Las características de Alloy pueden ser aprovechadas para establecer un enfoque que permita garantizar la calidad de los modelos de sistemas de software específicos.

Palabras clave: Alloy, DSL, Verificación

Contexto

Esta línea de Investigación, desarrollo e innovación (I-D-I) se inserta en el proyecto “Ingeniería de Software” coordinado por la a facultad de Ciencias Físico – Matemáticas y Naturales de la Universidad Nacional de San Luis (UNSL).

Introducción

Un *lenguaje específico de dominio* (DSL, por sus siglas en inglés) restringe sus primitivas a un problema específico con el objetivo de facilitar a los expertos el desarrollo de modelos [1]. Los DSLs tienen gran importancia dentro del enfoque *model driven architecture* (MDA) [2], ya que se utilizan para anotar modelos independientes de la plataforma, con el objetivo de transformarlos a uno o mas modelos específicos de la plataforma. De esta forma, siguiendo con la propuesta MDA, los modelos son sucesivamente refinados hasta obtener especificaciones cada vez mas concretas (código), alcanzando el producto final.

La verificación formal de los modelos en MDA permitiría incrementar la calidad del producto final. La verificación basada en métodos formales provee un poderoso mecanismo para detectar inconsistencias y chequear propiedades deseadas. Sin embargo, es infrecuente encontrar DSLs con herramientas que soporten la verificación formal de sus modelos, o que cuando lo hagan, esta verificación pueda ser complementada en sus aspectos menos fuertes.

Alloy [3] es un lenguaje formal, que incluye una amigable herramienta de *verificación y validación* (V&V) soportada por un analizador SAT. La especificación de una DSL en Alloy, permitirá aprovechar el potencial de Alloy para su V&V.

En trabajos anteriores, mostramos un enfoque basado en Alloy para la especificación, V&V de los aspectos estructurales que definen el metamodelo de un DSL [4,5]. Esto permite establecer una representación mas precisa del DSL propiamente dicho.

La línea de I-D-I propone un mecanismo general centrado en Alloy para la verificación de modelos y metamodelos específicos del dominio. Primero se valida y verifica el metamodelo de una DSL, y luego los modelos de esta. De esta forma, se extiende el enfoque en trabajos anteriores, ya que luego de realizar la V&V del metamodelo, nos centramos en desarrollar una guía para la verificación de sus modelos. El seguimiento de esta guía de habilitará la especificación de modelos más robustos, que llevará a la obtención de productos de software de alta calidad.

Líneas de Investigación, Desarrollo e Innovación

Los ejes de esta línea de I-D-I se detallan a continuación.

– La definición de una guía para la especificación y verificación con Alloy de modelos específicos del dominio. La guía debería establecer un proceso que indique cómo obtener una especificación Alloy que represente a la especificación en la DSL, y de qué manera éste debe ser verificado.

– La integración de métodos formales para la verificación de modelos específicos del dominio. Si bien, en su gran mayoría los DSLs carecen de una base formal que habilite su verificación, algunos de ellos presentan un sustento formal. En estos últimos casos, el enfoque propuesto debería integrar las técnicas y herramientas de verificación ya soportadas, con las que posee Alloy, potenciando la verificación formal de modelos específicos de dominio. El Analizador de Alloy, permite entre otras cosas, buscar instancias de los modelos, y detectar contraejemplos, utilizando la técnica Bounded Model Checking [6].

– La definición de casos de estudio. Diferentes casos de estudio permitirán testear la propuesta planteada. Esto es, una guía para la especificación, V&V de modelos específicos del dominio usando Alloy.

Resultados y Objetivos

En anteriores trabajos, planteamos llevar a cabo la especificación, validación y verificación del metamodelo de DSLs. Como caso de estudio tomamos a Archery – un lenguaje diseñado para el modelado, análisis y verificación de arquitecturas de software [7].

El objetivo de la presente línea de I-D-I es definir un mecanismo que permita obtener modelos en Alloy a partir de especificaciones en DSLs, utilizando el metamodelo de dicha DSL en Alloy (ya obtenido previamente), y permitiendo la V&V del modelo con el analizador.

Para llevar a cabo esta tarea, utilizaremos nuevamente como caso de estudio a Archery. Dada las características formales de este lenguaje, la especificación en Alloy puede potenciar la V&V, enriqueciéndola con los atributos que provee el analizador.

La verificación en Archery esta basado en un model checking exhaustivo, que analiza todos los estados posibles del sistema para chequear propiedades deseadas cuando ésta no es satisfecha. Sin embargo, los contraejemplos brindados por el fundamento formal de Archery son de difícil interpretación. Por otro lado, tiene asociado limitaciones tales como la explosión de estados, condicionando el

modelado sólo a la representación de sistemas de estado finito.

Por otro lado, Alloy lleva a cabo un bounded model checking; es decir, establece una aproximación de estados alcanzables hasta un límite determinado de antemano. Esto alivia el problema de la explosión de estados, y permite descubrir errores rápidamente, aunque no sea posible probar la ausencia de errores para todos los casos. Por esta razón, Alloy necesita ser combinado con otros métodos formales en la verificación de sistemas críticos, en donde el error debe ser totalmente descartado.

En la literatura, pueden encontrarse trabajos donde se muestra la conexión entre Alloy y otros enfoques formales [8, 9, 10, 11].

Entre los objetivos de la presente línea de investigación se incluye elaborar un marco de trabajo para explotar la integración de Alloy con otros métodos formales, que a su vez, sean los fundementos semánticos de DSLs. El framework debería indicar cómo utilizar Alloy combinado con el enfoque formal que soporte el DSL. Para llevar a cabo esta tarea, se deben caracterizar diferentes métodos formales con respecto a su integración con Alloy. De esta forma, dependiendo de la herramienta formal de la DSL, la guía permitirá integrar los enfoques.

Adicionalmente, se deben establecer otros casos de estudio que permitan fortalecer la propuesta aquí planteada. En este sentido, deben evaluarse diversas DSLs existentes en la actualidad.

Formación de Recursos Humanos

Dentro de la línea de investigación se desarrollan trabajos de tesis correspondiente al doctorado en Cs. de la Computación, Universidad Nacional de San Luis.

Referencias

[1] Arie van Deursen, Paul Klint, and Joost Visser. “Domain-specific languages: An annotated bibliography”. SIGPLAN Not., 35(6):26–36, 2000.

[2] OMG: MDA Guide, version 1.0.1, 2003.

[2] OMG: Meta Object Facility Core, v2.4.2, 2014.

[3] Daniel Jackson. Software Abstractions: Logic, Language, and Analysis. MIT Press, edición revisada, 2012.

[4] Ana Garis, Alejandro Sanchez. “Verification and Validation of Domain Specification Languages using Alloy”. Proceedings of the XXI Congreso Argentino de Ciencias de la Computación (CACIC 2015), ISBN 978-987-3724-37-4, pp. 589-598, 2015.

[5] Ana Garis, Alejandro Sánchez. "Especificación Formal de Lenguajes Específicos del Dominio utilizando Alloy", Proceedings of the XVII Workshop de Investigadores en Ciencias de la Computación (WICC2015), ISBN 978-987-633-134-0, id 6898, 2015.

[6] Edmund Clarke, Armin Biere, Richard Raimi, y Yunshan Zhu, “Bounded Model Checking Using Satisfiability Solving”, Journal of Formal Methods in System Design, Kluwer Academic Publishers, pp. 7-34, 2001.

[7] Alejandro Sanchez, Luis Barbosa y Daniel Riesco. “A language for behavioural modelling of architectural patterns”. Proceedings of the Third Workshop on Behavioural Modelling, pp. 17-24, 2011.

[8] M. Ferreira, S. Silva, and J. Oliveira. “Verifying Intel flash file system core specification”. In Modelling and Analysis

in VDM: Proceedings of the Fourth VDM/Overture Workshop, 2008.

[9] Paulo Matos, Joaão Marques-Silva. “Model checking Event-B by encoding into Alloy”. Proceedings of the First International Conference, ABZ. Volume 5238/2008, page 346. 2008.

[10] Renato Neves , Alexandre Madeira, Manuel Martins, Luís Barbosa. “An Institution for Alloy and Its Translation to Second-Order Logic”. In Integration of Reusable Systems: Advances in Intelligent Systems and Computing, Springer, pp 45-75. 2014.

[11] Miguel A Ferreira, Jose N. Oliveira, “Variations on an Alloy-centric tool-chain in verifying a journaled file system model”, Techn. Report DI-CCTC-10-07. 2010.